No title available.

Patent Number:	DE19615301
Publication date:	1997-10-23
Inventor(s):	HUBER KLAUS DR ING (DE); SCHEERHORN ALFRED DR ING (DE)
Applicant(s)::	DEUTSCHE TELEKOM AG (DE)
Requested Patent:	DE19615301
Application Number:	DE19961015301 19960418
Priority Number(s):	DE19961015301 19960418
IPC Classification:	G11B20/10 ; H04N5/91 ; H04N7/025 ; H04L9/32
EC Classification:	H04L9/32S, G11B20/00P, H04N5/913, H04N5/92N6, H04N5/926
Equivalents:	AU2386597, EP0894322 (WO9740496), A4, B1, WO9740496

Abstract

The invention relates to a method and a device for recording/ processing of authentic image and/or audio data. To achieve an authentic image or sound recording the entire process of converting from analogue to digital signals, the identification or the characteristics of the individual components used are received, and recorded or stored after a signature calculation. The digital data are linked with each other in a device shown by the figure in such a manner that separation of the individual processes is not possible on the device without manipulations which can subsequently be recognised. The signature also enables the order and the complete nature of all visual or audio information to be logged in a tamper-proof manner.

EL594612728US

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 15 301 A1**

(51) Int. Cl.[6]:
G 11 B 20/10
H 04 N 5/91
H 04 N 7/025
H 04 L 9/32

(21) Aktenzeichen: 196 15 301.8
(22) Anmeldetag: 18. 4. 96
(43) Offenlegungstag: 23. 10. 97

DE 196 15 301 A1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Huber, Klaus, Dr.-Ing., 64283 Darmstadt, DE;
Scheerhorn, Alfred, Dr.-Ing., 64293 Darmstadt, DE

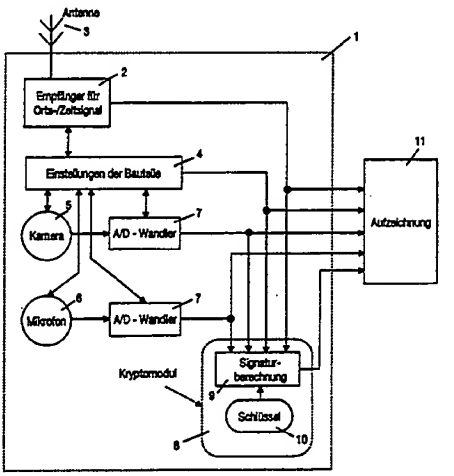
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	43 44 280 A1
US	52 67 314
US	51 36 646
US	50 97 504
EP	06 76 877 A2
EP	05 97 192 A2

RULAND,C.: Sichere Übertragung und Archivierung elektronischer Dokumente. In: DATACOM, 3, 1991, S.120-122,124,126,128,130;
SCHULTE,Heinz: Telekommunikation, Interest Verlag, Augsburg, Juni 1994, Bd.3, Teil 13, Kapitel 2.7, S.1-10, Kapitel 2.8, S.1-13;

(54) Verfahren und Vorrichtung zum Aufzeichnen/Verarbeiten von authentischen Bild- und/oder Tondaten

(57) Es wird ein Verfahren und eine Vorrichtung zum Aufzeichnen/Verarbeiten von authentischen Bild- und/oder Tondaten beschrieben. Zum Erreichen einer authentischen Bild- bzw. Tonaufzeichnung wird der gesamte Prozeß der Umwandlung von analogen zu digitalen Signalen, die Kennung bzw. die Charakteristika der einzelnen verwendeten Bauteile in eine Signaturberechnung mit aufgenommen, mit aufgezeichnet bzw. gespeichert. Die digitalen Daten werden in einer in der Fig. 1 dargestellten Vorrichtung so miteinander gekoppelt, daß eine Trennung der einzelnen Prozesse nicht ohne nachträglich erkennbare Manipulationen an der Vorrichtung möglich ist. Durch die Signatur werden auch die Reihenfolge und die Vollständigkeit aller visuellen bzw. akustischen Informationen fälschungssicher protokolliert.



DE 196 15 301 A1

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zum Aufzeichnen/Verarbeiten von authentischen Bild- und/oder Tondaten nach dem Oberbegriff des Patentanspruchs 1 bzw. des Patentanspruchs 7.

Analoge Aufnahme- und Übertragungsverfahren jedweder Art werden heute mehr und mehr durch digitale Verfahren ersetzt. Durch die Entwicklung der modernen Informationstechnik und der Digitalisierung wird die Manipulation der digitalen Daten immer einfacher. So können schon heute mit relativ geringem finanziellen und technischen Aufwand digital vorliegende Bilddaten bzw. allgemeine optische Informationen leicht mit entsprechender Soft- und Hardware gefälscht werden. Beispiele dieser Fälschungen gehen vom einfachen Kopieren von Daten, sowohl Bild- als auch Tondaten, Filmen oder deren Ausschnitte bis hin zur synthetischen Nachahmung von Fotografien oder Bildfolgen selbst für Experten. Für Experten ist es sehr schwer festzustellen, ob vorliegende Fotografien oder Filme authentisch sind, das heißt Abbild tatsächlich aufgetretener optischer Realitäten. Für bestimmtes vorgegebenes Tonmaterial trifft dieser Sachverhalt ebenfalls zu. Dies ist insbesondere dann wichtig, wenn zu Filmen oder Bildfolgen entsprechende Tonaufzeichnungen gemacht werden, wie bei Videoaufzeichnungen und Tonfilmaufzeichnungen allgemein üblich. Als Beispiel denke man sich Bildaufnahmen eines Unfallvorgangs, bei dem zum Beispiel die Ampelfarben manipuliert worden sind. Bei Aufnahmen eines Einbruchs könnte man auch die Gesichter der Täter austauschen und eventuell die dazu angeforderten Tonaufzeichnungen fälschen. Es sind bereits Verfahren zur Berechnung digitaler Signaturen unter anderem aus Kapitel 5, Stallings W., Network and Internetwork Security, IEEE Press 1995, ISBN 0-02-415483-0 und aus Kapitel 6, Stinson D.R., Cryptography: Theory and Practice, CRC Press 1995, ISBN 0-8493-8521-0 bekannt, die für eine gesicherte Informations- bzw. Datenübertragung verwendet werden.

In Zukunft wird die Synthese originalgetreuer Fälschungen von Bild- und Tondaten immer preiswerter und einfacher in der Handhabung. Die Originalität/Authentizität vorliegender digitaler Daten, insbesondere Bilddaten wird auf technischem Wege nicht mehr feststellbar sein, so daß Fälschungen bei den bisherigen Bild- oder Tonaufzeichnungen oder Kombinationen davon, leichter möglich werden. Durch eine Foto- oder Film- bzw. Videokamera werden Bilder, das heißt optische Signale, in analoge, elektrische Signale umgeformt, wobei letztere mittels eines Analog-Digital-Wandlers in digitale elektrische Signale transformiert werden, die dann gegebenenfalls aufgezeichnet werden. Der bisherige Lösungsansatz, die digitalen Daten mit einer digitalen Signatur zu unterschreiben, ist nicht hinreichend. Die digitalen Daten können zuvor gefälscht und erst danach signiert werden. Dieser Sachverhalt trifft auch für Tonaufzeichnungen zu.

Das zugrundeliegende Problem besteht darin, daß Bild- oder Tondaten bzw. deren Kombination in einer Art und Weise aufgezeichnet werden müssen, die sicherstellt, daß die Daten tatsächlich Abbild optischer Realitäten, zum Beispiel eines Einbruchs, und eventuell der zugehörigen Tondaten sind, das heißt nicht in irgendeiner Form manipuliert oder synthetisch erzeugt worden sind.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zu schaffen, die eine

authentische und integre Aufzeichnung/Verarbeitung von Bild- bzw. Audiodaten und eventuell dazugehörigen Tondaten, und deren fälschungssichere Speicherung und Wiedergabe vom Datenträger gewährleisten, so daß sichergestellt ist, daß die aufgezeichneten Daten nicht in irgendeiner Form manipuliert oder synthetisch erzeugt worden sind.

Die erfindungsgemäße Lösung der Aufgabe besteht im Kennzeichen des Patentanspruchs 1.

Für die erfindungsgemäße Vorrichtung ist die Lösung im kennzeichnenden Teil des Patentanspruchs 7 charakterisiert.

Weitere Merkmale bzw. Verbesserungen und/oder Ausgestaltungen der Erfindung sind in den Kennzeichen der restlichen Patentansprüche beschrieben.

Durch das erfindungsgemäße Verfahren bzw. die Vorrichtung wird erreicht, daß die Prozesse der Umwandlung der Bilder, das heißt optische Signale in analoge elektrische Signale einer Foto-, Film- oder Videokamera, die Umwandlung der analogen elektrischen Signale in digitale elektrische Signale mit Hilfe von Analog-Digital-Wandlern und die Berechnung einer digitalen Signatur über die digitalen Daten miteinander gekoppelt werden, so daß eine Trennung dieser Prozesse nicht ohne nachträglich erkennbare Manipulationen an der Vorrichtung möglich ist. Die Kopplung der Prozesse erfolgt in der Vorrichtung derart, daß eine Trennung nicht ohne nachträglich erkennbare Manipulationen möglich ist. Diese Kopplung kann physikalisch in der Vorrichtung derart erfolgen, daß die angegebenen Prozesse bzw. Prozeßschritte nur mit nachträglich feststellbarer Manipulation oder Zerstörung der Vorrichtung durch Unbefugte voneinander getrennt werden können und zwar deshalb, weil alle an den Prozessen beteiligten Bauteile bzw. Schaltungen in der gesamten Vorrichtung eingegossen sind oder durch Versiegelung der Vorrichtung geschützt sind.

Die Erfindung wird im folgenden anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher beschrieben.

Es werden folgende Bezugszeichen in der Beschreibung, der Fig. 1, in den Patentansprüchen und der Zusammenfassung verwendet:

1 Schaltung bzw. Vorrichtung zur geschützten Bild-/Tondatenaufzeichnung
2 Empfänger für Orts-/Zeitsignal
3 Antenne
4 Schaltung bzw. Speicher zur Kennzeichnung der Einstellung der Bauteile
5 Kamera
6 Mikrofon
7 A/D-Wandler
8 Kryptomodul
9 Signaturberechnung
10 Schlüssel
11 Aufzeichnung

Wie bereits erwähnt, muß zum Erreichen einer authentischen Bildaufzeichnung der gesamte Prozeß von den optischen Signalen bis hin zu den aufgezeichneten digitalen Daten nachvollziehbar, unwiderrufbar und beweisbar gestaltet werden.

Dies wird dadurch erreicht, daß die Prozesse der

— Umwandlung der Bilder, das heißt der optischen Signale in analoge elektrische Signale,
— Umwandlung der analogen elektrischen Signale

in digitale elektrische Signale durch Analog-Digital-Wandler und

– die Berechnung einer digitalen Signatur über die digitalen Daten in einer Vorrichtung 1 nach Fig. 1 miteinander so gekoppelt werden, daß eine Trennung dieser Prozesse nicht ohne nachträglich erkennbare Manipulation an der Vorrichtung möglich ist. Eine solche Kopplung der Prozesse kann beispielsweise physikalisch erfolgen, zum Beispiel durch Eingießen oder Verschließen der gesamten Vorrichtung oder durch Versiegelung der Vorrichtung.

Außerdem ist dann eine Modifikation der Vorrichtung zur Aufzeichnung authentischer Bilddaten erforderlich, wenn zum Beispiel die entsprechenden Tondaten mit aufgezeichnet werden sollen, wie dies zum Beispiel bei Tonfilmen der Fall ist. Die digitale Signatur wird dann erfindungsgemäß über alle audiovisuellen Daten gebildet, das heißt über die Daten, die von optischen Signalen stammen, und die Daten, die von akustischen Signalen stammen. Die Prozesse der Umwandlung der akustischen Signale in analoge elektrische Signale und deren Umwandlung in digitale elektrische Signale müssen dabei in der Vorrichtung 1 so mit den zuvor genannten Prozessen der Vorrichtung gekoppelt werden, daß eine Trennung dieser Prozesse nicht ohne nachträglich erkennbare Manipulation an der Vorrichtung möglich ist. Der Authentizitätsnachweis der digitalen Daten, das heißt der Nachweis, daß die digitalen Daten Abbild tatsächlich aufgetretener optischer bzw. audiovisueller Realitäten sind, erfolgt durch das Überprüfen der digitalen Signatur zu den vorliegenden digitalen Daten und durch das Überprüfen der Unversehrtheit der erfindungsgemäßen Vorrichtung.

Sind Manipulationen an der Vorrichtung zu erkennen, die vermuten lassen, daß die oben beschriebenen Prozesse getrennt wurden, oder paßt die digitale Signatur nicht zu den vorliegenden Daten, so werden die Daten als nicht authentisch abgelehnt.

Ist die Signatur jedoch korrekt, und die Vorrichtung 1 unversehrt, dann ist dadurch bewiesen, daß die vorliegenden aufgezeichneten Daten tatsächlich ein Abbild der optischen bzw. audiovisuellen Signale sind, die mit Hilfe der Vorrichtung 1 aufgenommen und gespeichert worden sind.

In diesem Zusammenhang ist es erforderlich, daß die Vorrichtung personalisiert ist. Das heißt, die digitale Signaturberechnung über die Daten erfolgt mit Hilfe eines geheimen Schlüssels 10, der

1. sicher in der Vorrichtung gespeichert ist und von außerhalb der Vorrichtung nicht in Erfahrung gebracht werden kann, ohne nachträglich erkennbare Manipulationen an der Vorrichtung 1, und
2. jeder Vorrichtung eindeutig zugeordnet ist, das heißt es gibt keine zwei Vorrichtungen mit gleichem geheimen Schlüssel 10.

Das Einbringen des geheimen Schlüssels 10 in die Vorrichtung 1 hat auf eine vertrauenswürdige, kontrollierte Weise zu geschehen.

Wäre die unter 1. genannte Bedingung nicht gegeben, das heißt der geheime Schlüssel 10 der Vorrichtung 1 ohne nachträglich erkennbare Manipulation der Vorrichtung 1 manipulierbar, so könnte nach dem Eruieren des geheimen Schlüssels 10 der Vorrichtung 1 die digitale Signatur zu beliebigen vorliegenden Daten berechnet werden. Diese Daten würden zusammen mit der unversehrten Vorrichtung 1 dann fälschlicherweise als authentisch anerkannt. Die unter 1. angegebene Bedingung ist deshalb unbedingt erforderlich.

Wäre die unter 2. angegebene Bedingung nicht gegeben, das heißt mehrere Vorrichtungen mit dem gleichen geheimen Schlüssel 10 würden existieren, dann könnten die Daten nur dann als authentisch anerkannt werden, wenn die Unversehrtheit aller dieser Vorrichtungen gewährleistet ist. Ist jeder Vorrichtung eindeutig jedoch ein Schlüssel 10 zugeordnet, so genügt die Unversehrtheit der entsprechenden Vorrichtung, um die mit dem ihr zugeordneten geheimen Schlüssel 10 unterschriebenen Daten als authentisch anerkennen zu können. Die Bedingung 2 ist deshalb sinnvoll, jedoch nicht unbedingt erforderlich.

In die Daten, die durch dieses Verfahren als authentisch nachgewiesen werden, können bzw. sollten neben den Daten, die von optischen bzw. audiovisuellen Signalen stammen, des weiteren Daten mit einfließen, die die Vorrichtung 1 bzw. die Einstellungen der Vorrichtung 1 identifizieren, beispielsweise

– Kamerakennzeichnung/-typ,
– bei audiovisuellen Aufzeichnungen zusätzlich Mikrofonkennung oder Typ,
– technische Aufnahmedaten, wie Blendeneinstellung oder Bildauflösung,
– bei audiovisuellen Aufzeichnungen zusätzlich Mikrofoncharakteristika,
– Typ des A/D-Wandlers bzw. der -Wandler,
– Abtastrate des A/D-Wandlers bzw. der -Wandler usw.

Falls ein vertrauenswürdiges Zeitsignal und/oder Ortssignal vorhanden ist, kann die Vorrichtung 1 zusätzlich mit einem Empfänger 2 für diese Signale ausgestattet werden. Das Zeit- und/oder Ortssignal wird dann mit aufgezeichnet und die digitale Signatur wird über die Daten, die von optischen Signalen stammen, sowie über das Zeit- und/oder Ortssignal und gegebenenfalls die zuvor genannten Einstellungen bzw. Kennungen der Vorrichtung 1 bzw. ihrer Bauteile 4 gebildet. Dadurch wird eine authentische Aufnahme von Bilddaten bzw. audiovisuellen Daten, zusammen mit authentischen Informationen über den Ort, die Zeit sowie die Einstellungen der Aufnahmevorrichtung und die Aufnahmevorrichtung selbst erreicht bzw. gewährleistet.

Das Einbringen des geheimen Schlüssels 10 in die Vorrichtung 1 auf eine vertrauenswürdige, kontrollierte Art und Weise erfolgt dadurch, daß Chipkarten bzw. Plug-In Module, in die bei einer vertrauenswürdigen Instanz der Schlüssel 10 programmiert wurde, verwendet werden. Des weiteren ist auf der Chipkarte bzw. im Plug-In Modul gewöhnlich auch das Verfahren zur Berechnung der digitalen Signatur implementiert. Dies hat den Vorteil, daß der Schlüssel 10 die Chipkarte bzw. das Plug-In Modul 8 nie verläßt und in der Chipkarte bzw. dem Plug-In Modul nicht von außen abfragbar, das heißt sicher gespeichert ist.

Ein prinzipieller Aufbau einer Vorrichtung 1, die in Form eines Plug-In-Moduls oder einer speziellen Chipkarte oder ähnlichem realisiert werden kann, ist in Fig. 1 dargestellt. Diese Schaltung 1 besteht insbesondere aus Schaltungen bzw. Speichern mit äquivalenten Daten zur Kennzeichnung der Einstellung der Bauteile 4, der Charakteristika einer Kamera 5 und gegebenenfalls eines Mikrofons 6, dazugehörigen A/D-Wandlern 7 und aus

einem Kryptomodul 8 mit Signaturberechnung 9 und Schlüssel 10. Außerdem kann gegebenenfalls ein Empfänger für Orts-/Zeitsignal 2 mit entsprechender Antenne 3 integriert sein. Dadurch wird die Sicherheit bzw. Authentizität der Aufzeichnung 11 noch erhöht. Das Gerät für die Aufzeichnungen 11 ist deshalb über entsprechende Leitungen mit dem Kryptomodul 8, den A/D-Wandlern 7, der Schaltung 4 und gegebenenfalls mit dem Empfänger 2 für das Orts-/Zeitsignal verbunden. In die Signaturberechnung gehen die Daten bzw. die Informationen, wie bereits beschrieben, aller vorhandenen Größen ein, weshalb die Signaturberechnungsschaltung 9 mit den A/D-Wandlern 7, der Kamera 5 bzw. dem Mikrofon 6 indirekt, der Schaltung 4 und dem Empfänger 2 verbunden ist.

Patentansprüche

1. Verfahren zum authentischen und integren Aufzeichnen/Verarbeiten bzw. Erstellen von authentischen und integren Bildern, gegebenenfalls mit dazugehöriger Tonaufzeichnung, sowie deren fälschungssichere Speicherung und Wiedergabe, **dadurch gekennzeichnet,**
daß über die digitalisierten Bildaten vor oder während der Aufnahme bzw. Aufzeichnung (11) eine digitale Signatur berechnet wird, die zusammen mit den digitalen Bilddaten gespeichert wird, und
daß der Prozeß der Umwandlung der optischen Signale in digitale elektrische Signale und der Prozeß der Berechnung der digitalen Signatur über die digitalen Bilddaten in einer versiegelten bzw. nicht öffenbaren Vorrichtung untrennbar miteinander gekoppelt werden.

2. Verfahren zur Erstellung von authentischen integren Aufzeichnungen langer Bildfolgen, wie zum Beispiel Filmen, dadurch gekennzeichnet, daß durch die Signatur die Reihenfolge und Vollständigkeit aller optischen Informationen fälschungssicher protokolliert wird.

3. Verfahren nach einem der Patentansprüche 1 oder 2, dadurch gekennzeichnet,
daß zur authentischen und integren Aufzeichnung audiovisueller Daten, wie zum Beispiel Tonfilmen, über die digitalisierten Bild- und Tondaten eine digitale Signatur berechnet wird, die zusammen mit den digitalen Bild- und Tondaten auf dem Träger der Aufzeichnung (11) gespeichert wird, und
daß der Prozeß der Umwandlung der optischen Signale in digitale elektrische Signale, der Prozeß der Umwandlung der akustischen Signale in digitale elektrische Signale und der Prozeß der Berechnung der digitalen Signatur über die digitalen Bild- und Tondaten in einer versiegelten bzw. nicht öffenbaren, verschlossenen Vorrichtung untrennbar miteinander gekoppelt werden und nicht von außen unfeststellbar manipulierbar sind.

4. Verfahren nach einem der Patentansprüche 1 bis 3, dadurch gekennzeichnet,
daß die digitale Signaturberechnung (9) über digitale Daten gebildet wird, die die Kennung der Vorrichtung (1), ihrer Bestand- bzw. Bauteile und/oder deren Einstellungen (4) charakterisieren und die in einem Modul, insbesondere einem Kryptomodul (8) erzeugt werden, das in die Vorrichtung (1) voll integriert ist und
daß bei unsachgemäßer bzw. manipulierter Handhabung Fehlfunktionen oder Teilstörungen ausgelöst werden.

5. Verfahren nach einem der Patentansprüche 1 bis 4, dadurch gekennzeichnet,
daß in die digitale Signatur digitalisierte Orts- bzw. Zeitdaten bzw. -signale von einem integrierten Empfänger (2) eingehen, der in die Vorrichtung (1) unlösbar voll integriert ist und
daß bei unsachgemäßer bzw. manipuliertier Handhabung Fehlfunktionen ausgelöst werden.

6. Verfahren nach den Patentansprüchen 1 und 2, dadurch gekennzeichnet, daß in die Signaturberechnungen (9) des Kryptomoduls (8) Kombinationen mindestens einer Schaltung bzw. eines Speichers zur Charakterisierung der Einstellungen der Bauteile (4) der Bild- und der Tonsignale bzw. deren Signalfolge eingehen und mit einem Schlüssel (10) gekennzeichnet werden.

7. Vorrichtung zur Durchführung des Verfahrens nach einem der Patentansprüche 1 bis 6, dadurch gekennzeichnet, daß die Vorrichtung (1) mindestens eine Schaltung bzw. einen Speicher zur Charakterisierung der Einstellungen der Bauteile (4), eine damit verbundene Kamera (5) mit A/D-Wandler (7), gegebenenfalls ein Mikrofon (6) mit A/D-Wandler (7) und ein Kryptomodul (8) mit Signaturberechnung (9) und Schlüssel (10) aufweist, und über Leitungen mit dem Gerät zur Aufzeichnung (11) zu einer Einheit integriert ist.

8. Vorrichtung nach Patentanspruch 7, dadurch gekennzeichnet, daß außerdem ein Empfänger für Orts-/Zeitsignale (2) mit zugehöriger Antenne (3) mit der Schaltung für die Einstellung der Bauteile (4), dem Kryptomodul (8) sowie dem Gerät zur Aufzeichnung (11) verbunden ist.

9. Vorrichtung nach einem der Patentansprüche 7 oder 8, dadurch gekennzeichnet, daß die Schaltung bzw. Vorrichtung (1) versiegelt ist oder in einem nicht öffenbaren Glas-, Kunststoff- oder Metallkörper fest integriert bzw. eingegossen ist.

Hierzu 1 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 196 15 301 A1
Int. Cl.[6]: G 11 B 20/10
Offenlegungstag: 23. Oktober 1997